



Methods and tools for GDPR Compliance through
Privacy and **D**ata **P**rotection **4** **E**ngineering

**Assurance methods
for data protection and privacy**

Project: PDP4E
Project Number: 787034
Deliverable: D6.4
Title: Assurance methods for data protection and privacy
Version: v1.0
Date: 08/08/2019
Confidentiality: Public
Author: Alejandra Ruiz (TEC)
Jabier Martínez (TEC)
Yod Samuel Martín (UPM)
Jacobo Quintáns (UPM)

Funded by



Table of Contents

DOCUMENT HISTORY	3
LIST OF FIGURES.....	3
LIST OF TABLES.....	3
ABBREVIATIONS AND DEFINITIONS.....	4
EXECUTIVE SUMMARY	5
1 INTRODUCTION	6
1.1 MOTIVATION	6
1.2 OBJECTIVE OF THE DOCUMENT	6
1.3 STRUCTURE OF THE DOCUMENT	6
1.4 RELATION WITH OTHER DELIVERABLES	6
2 ASSURANCE APPROACH FOR GDPR COMPLIANCE.....	7
2.1 THE ROLE OF SYSTEMS ASSURANCE IN PRIVACY AND DATA PROTECTION	7
2.2 MODELLING THE GDPR AS AN ASSURANCE REFERENCE FRAMEWORK	8
2.3 MODELLING ARGUMENTATION PATTERNS	11
2.4 MODULAR MODELLING	13
2.4.1 Integration of different regulations and standards.....	13
2.4.2 Integration of projects across the supply chain	14
3 METHODOLOGY FOR ASSURANCE.....	16
4 APPLICATION SCENARIO	19
4.1 GRAPHICAL MODELLING NOTATION	19
4.2 MODELLING GDPR AND ITS INTERPRETATIONS.....	20
4.3 MODELLING APPROACH AND PROCESS.....	22
4.4 MODEL OF ART. 35 DATA PROTECTION IMPACT ASSESSMENT.....	23
4.5 MODEL OF ART. 36 PRIOR CONSULTATION	30
4.6 MODELLING RISK CONTROLS THROUGH ARGUMENT PATTERNS	32
5 CONCLUSIONS	34
6 REFERENCES	35

Document History

Version	Status	Date
v0.1	Initial table of contents	05/06/2019
v0.3	Contributions from Tecnia are integrated	01/07/2019
v0.8	Contributions from UPM are integrated	06/08/2019
v0.9	Complete draft	06/08/2019
v1.0	Reviewers' comments are addressed	08/08/2019

Approval		
	Name	Date
Prepared	Alejandra Ruiz, Jabier Martinez (TEC)	06/08/2019
Reviewed	David Sanchez (Trialog)	06/08/2019
Reviewed	Yuliya Miadzvetskaya (KUL)	07/08/2019
Authorised	Antonio Kung	09/08/2019
Circulation		
Recipient		Date of submission
Project partners		08/08/2019
European Commission		09/08/2019

List of Figures

Figure 1. High-level process for data protection assurance.....	16
Figure 2. Reference Framework with the GDPR model.	21
Figure 3. Reference framework modelling of GDPR Art. 35.1 and 35.2 (detail).	24
Figure 4. Argumentation pattern for Art. 35.1.....	25
Figure 5. Reference framework modelling of GDPR Art. 35.4, 35.5, 35.6, 35.8 and 35.9 (detail).	26
Figure 6. Reference Framework modelling of GDPR Art. 35.7 and 35.10 (detail).	28
Figure 7. Argumentation pattern modelling different risks sources as per GDPR recital 75 (landscape oriented).....	29
Figure 8. Reference framework modelling of GDPR Art. 36.1, 36.2, 36.3 and 36.5 (detail).	32
Figure 9. Argument pattern about the NIST control SI-18.	33

List of Tables

Table 1. Main activities in the data protection assurance method.....	17
Table 2. Element icons in the Assurance Reference Framework metamodel	19
Table 3. Notation for relations in the Reference Framework Metamodel	19

Table 4. Notation of elements in GSN.	20
Table 5. Notation of relations in GSN.	20
Table 6. Codebook for annotation of Reference Framework and Argumentation Pattern elements and relations.	22
Table 7. Annotated text of GDPR Art. 35.1 and 35.2.	23
Table 8. Annotated text of GDPR Art. 35.3, 35.4 and 35.5.	25
Table 9. Annotated text of GDPR Art. 35.7 to 35.11.	26

Abbreviations and Definitions

Abbreviation	Definition
CoC	Code of Conduct
DPA	Data Protection Authority. Supervisory authority.
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECJ	European Court of Justice
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
GSN	Goal Structuring Notation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PDP4E	Privacy and Data Protection 4 Engineering
SDLC	Systems Development Life Cycle
SQA	Software Quality Assurance
SWEBOK	Software Engineering Body of Knowledge
WP	Work package
WP29	Article 29 Data Protection Working Party. See EDPB.

Executive Summary

Methods and tools for assurance (WP6) are highly related to the principle of accountability included in the GDPR (Art. 5.2). In this context of showing compliance, assurance methods can be considered as the “glue” of privacy data protection engineering outcomes, in the sense that the proposed assurance methodology should take into consideration the outcomes from methods and tools for data protection risk management (WP3), methods and tools for data protection requirements engineering (WP4) and methods and tools for data protection model-driven design (WP5), to be used for assurance purposes.

This document contains the proposed approach for GDPR from the assurance perspective including a methodology and its application. This preliminary description of the methodology for assurance proposed in the context of the PDP4E project, demonstrates how GDPR can be modelled as an assurance reference framework to assure compliance, and how privacy and data protection controls can be modelled as argumentation patterns whose instantiation will provide justified confidence to show such compliance. A detailed example of this approach is also illustrated by modelling parts of the GDPR and a selection of privacy controls.

The present document is the result of the first iteration. More insight will be provided during its validation in the context of PDP4E case studies. Also, the methodology will be improved and cover more areas not considered in this iteration.

1 Introduction

1.1 Motivation

The motivation of this document is to provide methodological guidance to the user concerning assurance while applying data processing activities and data protection methods. WP6 aims to provide support for the systematic capture, traceability and argumentation of evidence so as to demonstrate compliance with GDPR.

1.2 Objective of the document

The objective of this document is to include the contents of the method and descriptions of the data processing activities and data protection methods, and the models of the regulatory framework. The document tries to provide a methodological answer to the users' needs firstly identified in deliverable D2.2 [1] in relation with assurance and accountability. This is a first version of the specification of the privacy and data protection assurance method which will iteratively improve in the next iteration.

1.3 Structure of the document

This document is structured as follows: The current Section 1 is presenting a brief introduction of the document, Section 2 provides a description of assurance approach to GDPR compliance. Then, Section 3 describes the methodological process the user should follow when applying PDP4E approach for privacy assurance. Next, Section 4 includes the application scenario where the methodology has been applied using a preliminary prototype of the supporting tools to provide a database of assurance knowledge to be used in the case studies. Finally, Section 5 includes some conclusions of the work done.

1.4 Relation with other deliverables

This document is strongly related with deliverables D2.2 "Technical analysis and synthesis of user requirements" which has served as an input for Section 2.

Deliverable D6.1 "Specification and design of assurance tool for data protection and privacy" includes the design of the tool that will support the activities and the concepts described in this deliverable.

Also, this deliverable is strongly connected with the methods proposed in WP3, WP4 and WP5, as the outcomes of those WPs will serve as evidences of compliance. In Section 4 a preliminary connection with WP3 has been developed with an initial specification on a product-based argument pattern.

2 Assurance approach for GDPR compliance

2.1 The role of systems assurance in privacy and data protection

As defined by NATO Standard AEP-67 [2], *“System assurance (SA) is the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle”*. If we analyze this definition in detail, we may notice several relevant notions lying within. System assurance deals with vulnerabilities that may be exploited, which entails managing risks. In consequence, the definition does not mention e.g. undisputable formal proofs but a more subjective notion of **justified confidence**, which will for sure involve some degree of uncertainty (which will be acceptable up to a point depending on each specific case). Besides, such confidence is not blind trust, but “justified”, i.e. it is supported by well-grounded arguments, claims and evidences that help display the alignment of the system with the intended functions. Hence assurance is not focused on showing that the system exhibits some properties, but on demonstrating that there is a sound reasoning that allows claiming that those properties hold. Thus, assurance does not mean testing or validation, but it is one level above those: the assurance process may, of course, demand that testing or validation activities be carried out, and use their results as evidences, but the assurance process does not get into the details of the execution of such tests. Further, assurance activities shall cover the **whole life cycle** of a system (not only testing or validation). For example, an assurance process may specify that potential users have been involved during the requirement capture, or that they have been trained before operating the system.

All this implies that **assurance shall be systematically planned beforehand and carried out according to such plan**, whose activities go in parallel to those of other disciplines (e.g. design, validation, coding) within the Systems Development Lifecycle (SDLC). Thus, according to the mentioned NATO standard, *“This confidence is achieved by system assurance activities, which include a planned, systematic set of multidisciplinary activities to achieve the acceptable measures of system assurance and manage the risk of exploitable vulnerabilities”*. More restrained, qualified definitions of assurance which apply only to a given industry or category of requirements are similarly focused on that aspect of establishing a systematic process. SWEBOK 3.0 [3] states that *“software quality assurance (SQA) is a set of activities that define and assess the adequacy of software processes to provide evidence that establishes confidence that the software processes are appropriate and produce software products of suitable quality for their intended purposes”*. Or, with regards to safety requirements, the EU regulations 2096/2005 [4] and 1035/2011 [5] define safety assurance as *“all planned and systematic actions necessary to afford adequate confidence that a product, a service, an organisation or a functional system achieves acceptable or tolerable safety”*.

System assurance always depends on the definition of what are the system “intended functions”, which may also encompass ‘non-functional’ aspects; indeed, this concept has been heavily used in critical systems from the perspective of requirements which are subject to uncertainty constraints, e.g. safety requirements, cybersecurity, and we are applying it here to Privacy and Data Protection.

Regarding GDPR, we encounter that Art. 5.2, when describing data protection principles, states that *“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”*, where said paragraph 1 defines other data protection principles (e.g. transparency or minimisation). That is, in order to comply with GDPR, we can say that it is

not enough to behave well, but you also need to demonstrate that behaviour so as to be above suspicion and generate trust. As a matter of example, records of written consent from the data subjects shall be kept by the controller (Rec. 42, Art. 7.1) in order to be able to demonstrate that they did provide their consent, and that it was voluntary, informed, etc. Likewise, records of processing activities are also required (Art. 30, except for small organizations) and can be requested by supervisory authorities. Systems assurance responds to that need and can hence become pivotal to support this **accountability principle**, as its activities are precisely aimed at providing evidence and argumentations that support the claims of compliance with a given intended specification.

Assurance is also useful to meet other contents of GDPR. For instance, available evidences can be leveraged to provide transparent information to the data subjects under different circumstances (Art. 12, Rec. 60, Rec. 85) and hence support the transparency principle (Art. 5.1.a and Rec. 39, Rec. 58, Rec. 78), or to be used to claim adherence to codes of conduct (Art. 40), or provide proofs for certifications (Art. 42), and even to provide the notifications required after data breaches (Art. 32, Art. 33).

Last, the fact that assurance supports the existence of a view of the system status with respect to compliance and how it has been reached, is key for two data protection goals (as defined by Hansen [6]): transparency (*"all privacy-relevant data processing –including the legal, technical, and organizational setting– can be understood and reconstructed at any time."*) and intervenability (*"intervention is possible concerning all ongoing or planned privacy-relevant data processing"*), which can in turn be mapped to traditional management disciplines of monitoring and control.

2.2 Modelling the GDPR as an assurance reference framework

Systems assurance, as an engineering process and from the engineering perspective, can provide support to compliance with privacy and data protection normative frameworks. But then, the first step shall consist in modelling such normative framework, which is called, in systems assurance parlance, the "Reference Framework". **Reference Frameworks** are modelled according to a predefined metamodel. In PDP4E we selected the Common Assurance and Certification Metamodel (CACM) [7], which is specific from the OpenCert tool, yet available as open-source software. This Reference Framework model contains definitions of processes that may/shall be followed according to the regulation, as well as formal requirements. As a regulation is common to many projects, the Reference Framework needs to be created and then reused in any project. Then, during the execution of a project by an organization, the project will generate evidences which can be traced to the model of the reference framework, and which allow asserting compliance with it through argumentations of compliance. Details about this process is available in the description of the assurance use cases available in D6.1 [8].

A Reference Framework contains definitions of activities that shall be carried out, roles who perform them, and artefacts that are used as either inputs or outputs thereof. Besides these three main elements, there are other elements that may appear in a Reference Framework, of which we will only highlight some which are relevant in the context of GDPR. All the quoted citations come from the above mentioned reference [7].

- **Activities** are *"units of behaviour that a reference assurance framework defines for the system lifecycle and that must be executed to demonstrate compliance"*. As presented in section 6.3 of D2.3, GDPR contains implicit or explicit definitions of multiple "tasks", which we may

roughly map now to the Activities in the systems assurance method. Depending on their relationship with systems assurance, we may roughly classify those activities into:

- **Data processing activities** (as defined in Art. 4) which represent the scope of application of GDPR. That is, they are not the activities required by GDPR as a normative framework as such, but the activities about which GDPR establishes a set of requirements that shall be assured.
- **Data protection activities during the design and development stage:** following the Data Protection by Design principle, GDPR specifies a number of activities to be carried out during the development of a system to e.g. record processing activities (Art. 30), assess risks through DPIAs (Art. 25, 26 and related activities), implement technical and organisational protection measures or controls (Art. 24), choose processors (Art. 28), or abide by external rules (certifications, codes of conduct, etc.)
- **Data protection activities during the operation stage:** GDPR sets many activities that shall be carried out during the operation of a system in order to support data protection, e.g. record consents from data subjects, honour the rights of the data subjects when requested to do so, etc. Instances of such activities can be carried out once per data subject, processing activity, purpose, and even category of personal data. The systems assurance does not address each instantiation of the activity, but other enabling activities that precede them during the development process. For instance, systems assurance would not evaluate whether a consent is recorded, but whether an appropriate consent recording system has been integrated.
- **Others:** GDPR sets the conditions which data processing activities shall keep to, without prescribing specific activities e.g. ensuring the lawfulness of processing and purpose limitation or compatibility (Art. 6), keeping integrity of personal data, etc. Unspecified techniques shall be applied to ensure these requirements are abided by.

Different relationships between Activities of a Reference Framework can be defined:

- **Preceding Activities:** An Activity can have zero or more preceding activities, which must be executed before. Note that implicit precedence activities may also exist due to indirect dependencies through input artefacts which shall have been output by other activities.
- **Subactivities:** An Activity can be composed of any number of sub-activities, which provide a more fine-grained description. Precedence relationships may be defined (but they are not required) between such sub-activities.
- **Artefacts** correspond to *“the types of units of data that a Reference Assurance Framework defines and that must be created and maintained during system lifecycle to demonstrate compliance”*. An artefact can represent any type of entity which can be captured as evidence in the assurance process. Examples of artefacts are a document, a model, a software installation, a database record, etc.

Artefacts are related to Activities in several ways:

- **Produced Artefacts** are generated (or changed) by the execution of an activity.
- **Required Artefacts** are necessary for the execution of an Activity. A given Artefact can be both Produced and Required with respect to an Activity (e.g. if such activity updates the Artefact to a newer version).
- **Constraining Requirements** represent indirect relations between Activities and Artefacts, mediated by a Requirement, as detailed below.

- **Roles** represent the agents who execute an Activity; each role in the model shall be linked to the Activities it is involved in. Most of the times that GDPR defines or refers to a given Activity, it specifies which party is responsible for carrying them out. Some of these roles are quite usual throughout the GDPR, e.g. [data] controller, [data] processor, supervisory authority, data subject, data protection officer. It may happen that several Roles intervene in a single activity (each with a different responsibility); in particular, in GDPR it is common that a given party is required to consult or get advice from another one when carrying out an activity. Those ‘advisor’ or ‘help’ roles are modelled as intervening in the Activity as well.
- **Requirements** are “*criteria (e.g., objectives) that a reference standard defines (or prescribes) to comply with it.*”, which may in turn be related to one another. On the one hand, a Requirement can be owned by an Activity, meaning that it must have been met by the end of the Activity execution; on the other hand, an Artefact may have such Requirements as constraining requirements, meaning that the existence of such Artefact satisfies them. In summary, the relation between Activities, Artefacts and Requirements goes as follows: If an Activity owns a Requirement, then there must be an Artefact (created by that Activity or by another one) which shows it as a constraining requirement.
- **Applicability and Criticality Levels:** Not all the clauses of a given standard need to be applied at each and every context. It may be the case that, e.g. a clause only refers to specific technologies or industries. Then the clause would have nothing to say about projects which do not use such technology (or are not applied in that industry, respectively). Likewise, it may be the case that some clauses shall only be enforced in systems which deal with especially critical matters. In systems assurance, this is modelled by defining different Applicability Levels and Criticality Levels within a standard, which can then be used to qualify the scope of application of Requirements.

Examples of applicability levels can be found throughout the GDPR. GDPR provides some exemptions for small organizations, it establishes specific requirements when data is being transferred to third countries, etc. Criticality is less common, but there are instances still. For example, special categories of personal data (e.g. genetic or religious beliefs) cannot be processed on the same grounds as any other data. For special categories their processing is prohibited according to the GDPR unless some conditions listed in Art. 9 paragraph 2 are met. Also, special groups of data subjects (i.e. minors) are subject to special protection, or special processing activities (e.g. profiling, direct marketing) require specific provisions. A detailed list of GDPR clauses where such variability may appear has been compiled by Hoepman and Colesky, who have included it in an online available tool¹. Another source for differences in applicability of parts of GDPR are the opening clauses which leave room for some aspects to be regulated at national level, and which hence depend on the Member State of the roles involved; a detailed discussion of such opening clauses of GDPR has been compiled by Kühling et al. [9] and they also provided a comprehensive graphical summary about the opportunity to do things in a different way across Member States regarding the GDPR².

From the perspective of a Reference Framework, we talk about ‘reference’ activities, artefacts, and roles, as they represent abstractions, which are then materialized in each project as concrete,

¹ Privacy patterns selection tool <https://privacypatterns.cs.ru.nl/tool/>

² Graphical summary of “Member States’ room for manoeuvre in the GDPR”, <https://www.flickr.com/photos/winfried-veil/29706462112/>

specific instances of those. In order to ease the modelling of the Reference Framework, it is supported by a visual notation [7], presented in Section 4.

2.3 Modelling argumentation patterns

The Reference Framework model provides a graph of Activities, directly related through composition and precedence relations, and indirectly through Artifacts and Requirements. However, it does not provide for the explicit definition of conditionals or branches in the process. These are modelled through a different perspective that comes into play here: that of argumentation patterns.

When an assurance project is carried out (alongside an overall development project), their results are captured in an assurance case, i.e. *“A reasoned and compelling argument, supported by a body of evidence, that a system, service or organisation will operate as intended for a defined application in a defined environment.”* [10], where an argument is defined as *“a connected series of claims intended to establish an overall claim”*. That is, to achieve the justified confidence mentioned at the beginning of this section, a series of claims are asserted, and related among one another to build a compelling argument. Arguments ultimately hold several evidences, through a graph of elements that represents the ‘reasoning’ that helps deriving the argument.

These arguments are built when an assurance project is enacted; however, usually similar arguments are used once and again to justify compliance with a given normative framework. This reuse can be captured through argument patterns. Argument patterns are abstractions of argumentations which provide hints on how to prove compliance with (part of) a reference framework by instantiating the pattern during project enactment.

An **argumentation** may consist of:

- A **top-level claim** to be proved, represented as a **top-level goal** (the requirement of being compliant with the part of the standard).
- Successively refined **supporting sub-claims** which all together support a higher-level claim.
- **Strategies** that associate claims to their sub-claims, and which represent the inference process that supports the higher-level claim (e.g. as all the sub-claims hold).
- **Evidences** that directly support a given claim by providing a **solution** to it, and which are the leaf nodes in the argumentation hierarchy.
- Elements in the context where claims and strategies are asserted: proper **context** where a claim or strategy is considered (effectively constraining its scope), **assumptions** that must hold for claims or strategies to be valid (acting as prerequisites that need not be substantiated), and **justifications** that explain why they are acceptable. Such contextual elements should not be contradicted by any element of the argumentation.

An **argumentation pattern** may include such elements plus others that help model the structural and element abstraction (as the argumentation pattern does not provide a closed argument, but a partial argument to be completed during pattern instantiation):

- **Uninstantiated elements** which allow specifying abstract templates of claims / strategies / evidences that need to be instantiated for each assurance case.
- **Undeveloped elements** which leave part of an argumentation tree incomplete, to be later (during project enactment) developed through further supporting claims and evidences.

- **Optionality** applied to a single relationship between claims / strategies / evidences, and which mean that, in an assurance case, valid arguments can be created both with or without instantiating such relationship.
- **Multiplicity** also applied to a single relationship, which mean that an assurance case can contain a given (bounded or unbounded) number or instances of such relationship.
- **Options** applied at once to several relationships with a common source and different destinations (e.g. from a claim to a set of sub-claims), and which mean that one of them can be chosen to support the higher-level element in the assurance case. Options need not be 1-of-n, they can also be qualified with other bounds.

Models of arguments and argumentation patterns can be represented through a visual notation [7][10], known as the Goal Structuring Notation (GSN), and introduced in Section 4.

Argumentation patterns can be included at different stages of an assurance project. A first use we discuss here is related to the use of contextual elements to model **conditional clauses** appearing in the regulatory framework, and which cannot be determined before the assurance case is developed. This distinguishes such argumentation contextual elements from the applicability and critically levels above discussed (which can be determined as soon as the project scope is determined).

GDPR contains several conditional clauses which constrain when an action is or not required. For instance a DPIA shall be carried out *“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. [...]”* (GDPR, Art. 35.1) From an assurance perspective, this clause entails that:

- 1) Artefacts which define the nature, scope, context and purposes of the processing shall have been elicited somehow (as they shall be taken into account).
- 2) An activity shall be carried out to estimate whether of that processing is likely to result in a high risk (even if this is just an initial appraisal, note that the output is not a detailed risk evaluation, but just the likelihood of such risk existing).
- 3) If such high risk is likely, then a DPIA activity shall be carried out in order to reach compliance with that clause (that DPIA will be surely composed of other sub-activities).
- 4) Otherwise, compliance is justified by the fact that the likelihood is low.

That is, in this example, an argumentation pattern can be created with two options to justify compliance: a) the execution of a DPIA or b) a low likelihood result in the initial risk appraisal.

When the assurance project is enacted, only one of those branches of the argumentation pattern will be chosen and included in the arguments of the particular assurance case (either the DPIA has been carried out or a low risk likelihood has been appraised). Note that this does not prevent a DPIA from being carried out for any other reason, but just that compliance can be claimed even when it does not exist.

Argumentation patterns can be created to ease the process of demonstrating compliance with similar clauses, which appear all over GDPR. Likewise, other argumentation patterns will be created to appropriately model other structures in the regulatory framework that cannot be easily captured by the modelling of the normative framework.

A second use of argumentation patterns is related to **security and privacy controls**, i.e. “A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.” or “the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII [Personally Identifiable Information]” [11]. Security and privacy controls can be established as the result of requirements engineering and/or risk management activities (following a goal-driven or a risk-oriented approach, respectively). Those controls act as solution-oriented requirements, in that they determine the design mechanisms, and realise the technical and organizational measures required throughout GDPR (and especially in Art. 24, 25, 35 and 36).

Engineers may choose controls from catalogues or knowledge bases that they have at their disposal, and which will have been modelled beforehand (as part of e.g. an organizational-wide endeavour, or provided by external specialist firms, or from external catalogues). That model of a security/privacy control may also contain an argumentation pattern which specifies which evidences are expected to demonstrate that a control has been implemented. For instance, the implementation of SSL as a mechanism for secure communications is supported by the existence of a valid certificate and a specific server configuration.

A different approach that can be explored to model controls is based on the use of ‘techniques’, which in systems assurance represent different approaches that can be applied to address the same activity. While argumentation patterns are only provided as potential alternatives to comply with a standard (which leaves room for other approaches), applicability tables can be employed to model the use of controls that are explicitly required by a given standard. A standard can prescribe the application of specific techniques, especially when a given applicability or criticality level holds (as expressed in technique applicability tables).

2.4 Modular modelling

Unless a development project has trivial contents, it will be typically needed that assurance cases are addressed in a modular way, from both the perspective of the reference framework specifications and that of the system components. That is where modularity in systems assurance comes into play. Modularity aspects are not still implemented in this phase of the project, but we advance here their relationship with GDPR and how they are planned to be addressed.

2.4.1 Integration of different regulations and standards

In an assurance project, it may be the case that different PDP regulations and standards are applicable. The basic regulatory framework consists of GDPR plus its interpretation through WP29/EDPB guidance and ECJ rulings. However, GDPR itself anticipates how it can be extended with codes of conduct, certifications, binding corporate practices, or even Member State law in some cases. Besides, there are data protection standards which provide techniques to operationalize parts of GDPR. For instance, GDPR requires that a DPIA is carried out but it does not prescribe how to do it. On the contrary, ISO 29134 provides a detailed method to carry it out. Or, GDPR mandates that security and privacy technical and organizational measures are introduced in the systems, but it does not tell which, when, where or why. This is addressed by e.g. NIST 800-53 [11] or ISO/IEC 27552 [12] (just published, and which provides the privacy counterpart to ISO/IEC 27002 with respect to security controls). Besides, organizations may establish their own, internal standards, corporate policies, development process models, etc.

Within the realm of systems assurance, such integration of different standards is addressed through '*equivalence mappings*'. An equivalence mapping is a map between elements of different standards (usually including requirements, artefacts, and activities; potentially also roles and techniques), so that compliance with an element in the source standard implies compliance (or partial compliance) with another element from the target standard. Then, during the execution of an assurance project, artefacts created to comply with one source standard can be reused and be also mapped to the target standard (through a '*compliance map*').

Of course, an equivalence mapping between different standards seldom yields a perfect direct map:

- The equivalence mapping is usually just a partial map (not all the elements from one standard are included in the other).
- A mapping may entail the introduction of post-conditions ("*mandatory extra activities, not included in the standard, that must be performed in case of reusing the target element*" [13]).
- Interpretations may be needed which add to the trace from the elements of the source standard to those of the target.

Besides all that, even a single standard can be decomposed into different modules (reference frameworks, argumentation patterns) which include references from one another, to simplify the modelling of the reference framework and its instantiation.

2.4.2 Integration of projects across the supply chain

It may be the case that a project is composed of the results of different sub-projects, each creating their own subsystem, and potentially following a different process and even being executed by different teams. From the GDPR perspective, this is especially relevant when there are different participants involved in the supply chain of data processing activities, as it is the case of:

- data processors which "*process data on behalf of a controller*" (as defined in Art. 4.8) and with specific obligations (established in Art. 28);
- joint controllers which "*jointly determine the purposes and means of processing*" (Art. 26);
- and groups of undertakings (including controller—controlled organizations, but also in practice involving "*institutions affiliated to a central body*", or "*group of enterprises engaged in a joint economic activity*") which can arrange binding corporate rules (Art. 47, Rec. 110).

Besides, GDPR includes throughout its text some other special considerations that apply to each of these supply chain agents.

In systems assurance, this integration is addressed by modular assurance cases. An argumentation can be packaged as a module which exports some elements (goals, solutions, or contexts) labelled as public. Then another argumentation can import in turn the former, and include: 1) references to the imported module argument as a whole, as well as 2) away-elements (away goals, solutions and contexts) that represent pointers to the respective public elements³ that lie in external, imported modules. Whole modules can also be linked through the same relations that are used between individual elements (SupportedBy and InContextOf).

³ Away elements can be used in place of their respective local elements; but away-goals can also be used in replacement of local justification elements.

Another level of indirection can be achieved through contract modules. A contract module provides links between two other modules (one providing claims that support the argumentation of the other). This contract can develop goals which are not explicitly developed in a given (target) module, and which are labelled as “to be supported by contract”.

It shall be noted that the integration between different subsystems can likewise be far from perfect, as emergent synergies or conflicts may appear when different subsystems are integrated. To deal with that, there is a concept called ‘agreement’ (which can be supported by the use of an agreement argumentation pattern) that justifies why connecting modules makes everything work. Besides, an assurance case can be created for the integration process itself.

3 Methodology for assurance

In the following Figure 1 we can see the high-level process for data protection assurance. As reader can see, two main activity flows are part of the data protection assurance process.

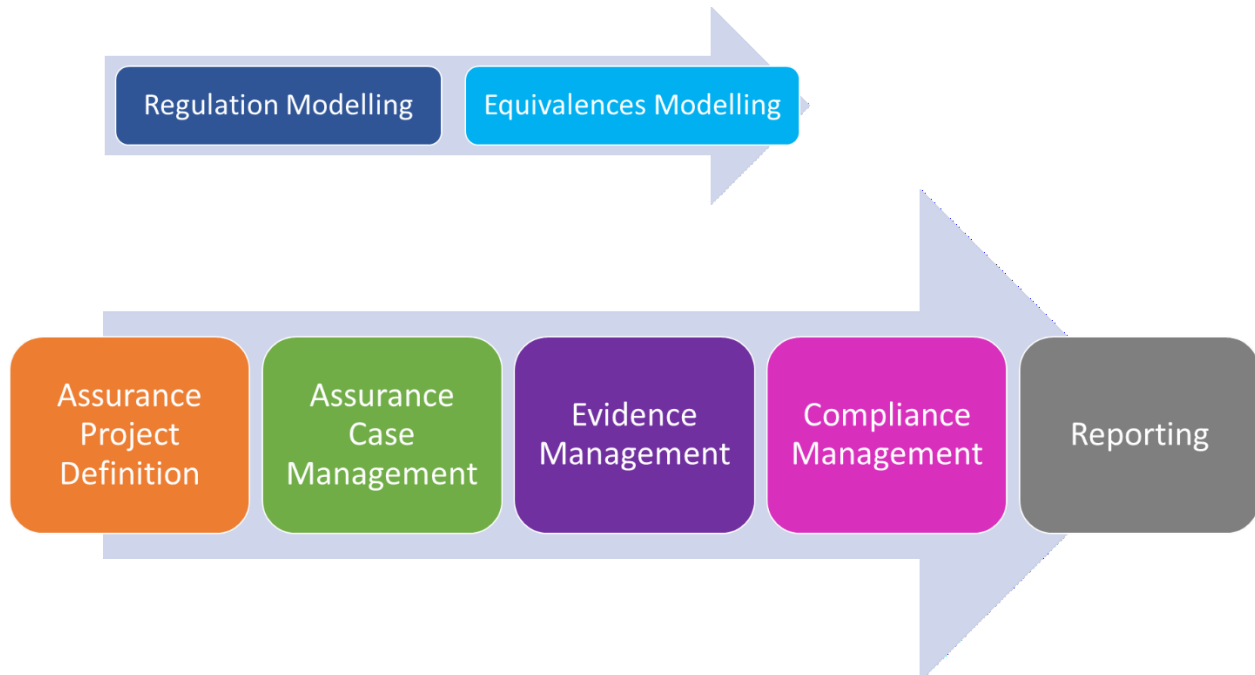


Figure 1. High-level process for data protection assurance.

On the one hand, a model of the regulatory framework whose compliance is to be assured shall be created. In our case, the regulatory framework will be GDPR, but it can also include WP29/EDPB guidance, data protection standards, corporate policies, etc., as well as their mapping to GDPR when possible. This model may contain definitions of processes that may/shall be followed according to the regulation, as well as formal requirements.

This modelling is addressed by regulation modelling and equivalence modelling; two activities that are done with independence of the execution of a given project. A model of the regulatory framework needs to be created only once, and then it can be reused in further projects: indeed, PDP4E will provide a model of GDPR itself; nonetheless, an organization may need to model other privacy and data protection standards (e.g. industry-specific) they will abide by. The equivalence modelling activity is an optional activity and should be performed only if the equivalences from at least two different regulation models are identified and both regulations are of interest for the organization.

On the other hand, the assurance project execution includes the activities of assurance project definition, assurance case management, evidence management, compliance management and reporting. It shall be done once the regulation is modelled as all the compliance activities rely on this modelling. First, when an assurance project is started, a baseline model needs to be defined, answer questions such as abidance with which standards the project is targeting, which are the relevant applicability and criticality levels (if any), etc. Then, when the organization carries out the processes (e.g. development of a product, operation of a service), ‘evidences’ must be generated and collected. These evidences can come from different types of artefacts generated by any other process including, e.g. results of risk evaluation, requirements traceability, validation or verification, but also annotated system architecture models themselves. These evidences are stored, together with traceability information that maps them to the model of the normative framework (to which reference artefact each evidence responds). These evidences are

linked through previously defined argumentations to demonstrate compliance, which are generated by instantiating argumentation patterns or by generating ad hoc argumentations for the current project.

Table 1. Main activities in the data protection assurance method.

	Activities	Roles	Work products
Regulation Modelling	Project-independent activities. It should be done just one by the company once a standard, regulation, guidance, code of conduct or best practices are published. Capture, digitise, store and retrieve standards compliance knowledge.	Standards' expert, Process Engineer	<i>Input:</i> GDPR, codes of conduct, DPA guidance, implementation standards (e.g. ISO 29134), company practices. <i>Output:</i> Standards model using OpenCert Reference Framework model Assurance patterns derived from standards
Equivalence Modelling	Project-independent activities. Map the equivalence between the elements (roles, activities, artefacts, requirements) of two of regulation's models (e.g. GDPR articles about DPIAs with ISO 29134)	Standards' expert, Process Engineer	<i>Input:</i> Two standards modelled using OpenCert Reference Framework model <i>Output:</i> Equivalence mapping model
Assurance Proj. Definition	Define the scope of compliance for a project, project compliance lifecycle, and compliance means.	Assurance Manager (e.g. Privacy Manager) (Plus, Process Engineer acting as Assurance Manager)	<i>Input:</i> Reference Framework Dev. Project Scope Definition <i>Output:</i> Assurance Project Baseline model
Assurance Case Management	Define argumentation using compliance arguments and product arguments.	Security & Privacy Assurance Developer / Engineer	<i>Input:</i> Assurance Project <i>Output:</i> Assurance Case

	Activities	Roles	Work products
Evidence Management	Collects all the project artefacts, and trace them for assurance accountability purposes	Assurance Developer / Engineer	<i>Input:</i> Assurance Project Artefacts (models, design, control implementations, etc. used as evidence during the development lifecycle) <i>Output:</i> Evidence Model
Compliance Management	Maps the actual evidence generated during the project development with the standard compliance requirements.	Assurance Manager DPO	<i>Input:</i> Baseline Assurance Case Evidence Model <i>Output:</i> Set of Compliance maps
Reporting	Provides information in a human-readable way about the status of the project compliance with regards to the standard requirements.	Assurance Manager DPO	<i>Input:</i> Baseline Compliance maps <i>Output:</i> Compliance report Metrics

4 Application scenario

4.1 Graphical modelling notation

As explained in the previous section, the first activity that should be performed according to the methodology proposed in section 3 above is the regulation modelling. This modelling activity is supported by the use of a prototype of the OpenCert assurance tool, which provides an editor to create models through a graphical notation, supplemented with textual forms to edit those fields which are not represented visually. Model elements of the reference framework are rendered as rectangular boxes with their name in it, decorated with icons that indicate the element type; while relations between two elements are shown as arrow lines with different colours and arrow heads, as detailed in Table 2 and

Table 3.

Table 2. Element icons in the Assurance Reference Framework metamodel








Icon	Element
	Activity
	Role
	Artefact

Table 3. Notation for relations in the Reference Framework Metamodel

Line/arrow	Relation (origin and source)
	Input (Artefact to Activity)
	Output (Activity to Artefact)
	Participation (Role to Activity)
	Precedence (Activity to Activity)
N/A (box within box)	Containment (Activity to Activity)

The standards modeler can resize element boxes and distribute them on a bidimensional canvas at their will. Sub-activities are represented graphically by embedding the sub-activity rectangle within that of the 'parent' activity (appropriately enlarged). Other elements not detailed above (e.g. Requirements, Applicability and Criticality Levels) and the respective relations shall be modelled by manually entering the details in model edition forms provided by OpenCert as well. Besides, free-text annotations can be attached to any element or relation, represented by a yellow-shaded rectangle (mimicking the appearance of a sticky note).

Regarding the argumentation patterns, they are also supported by a graphical notation known as Goal Structuring Notation [10]. In this case, the different element types are not distinguished

by an icon but by the shape of the box. Table 4 and Table 5 shows the notation for elements and relations⁴.

Table 4. Notation of elements in GSN.







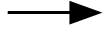
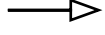
Shape	Element
	Goal
	Strategy
	Solution
	Context
	Justification
	Assumption

Table 5. Notation of relations in GSN.

Line / arrow	Relation (origin and source)
	Supported by (from goal to goal / strategy / solution, or from strategy to goal)
	In context of (from goal / strategy to context / assumption / justification)

4.2 Modelling GDPR and its interpretations

In the rest of this section, we will show how the GDPR can be modelled as an OpenCert reference framework and argumentation patterns, as introduced in section 2. With that aim, and in order to create a knowledge database with assurance information, we have started modelling the GDPR as a reference framework. More specifically, herein we exemplify it with the contents of the Article 35, which deals with the Data Protection Impact Assessments (DPIA) that controllers shall carry out when a processing may entail high risks to data subjects, and Article 36, which deals with the consultation that controllers shall perform with supervisory (data protection) authorities if the results of the DPIA still yield high residual risks. This is supplemented with the analysis of the recitals respectively related to those articles, plus the contents of WP29 guidance [14] which provides interpretive details of Data Protection Impact Assessments should be addressed. Figure 2 shows the results of this modelling, which we will discuss in detail below, together with the process to elaborate such model.

⁴ Adapted from Goal Structuring Notation Community Standard Version 2 by The Assurance Case Working Group (ACWG), available at <http://scsc.uk/SCSC-141B>, licensed under CC-BY-4.0 license

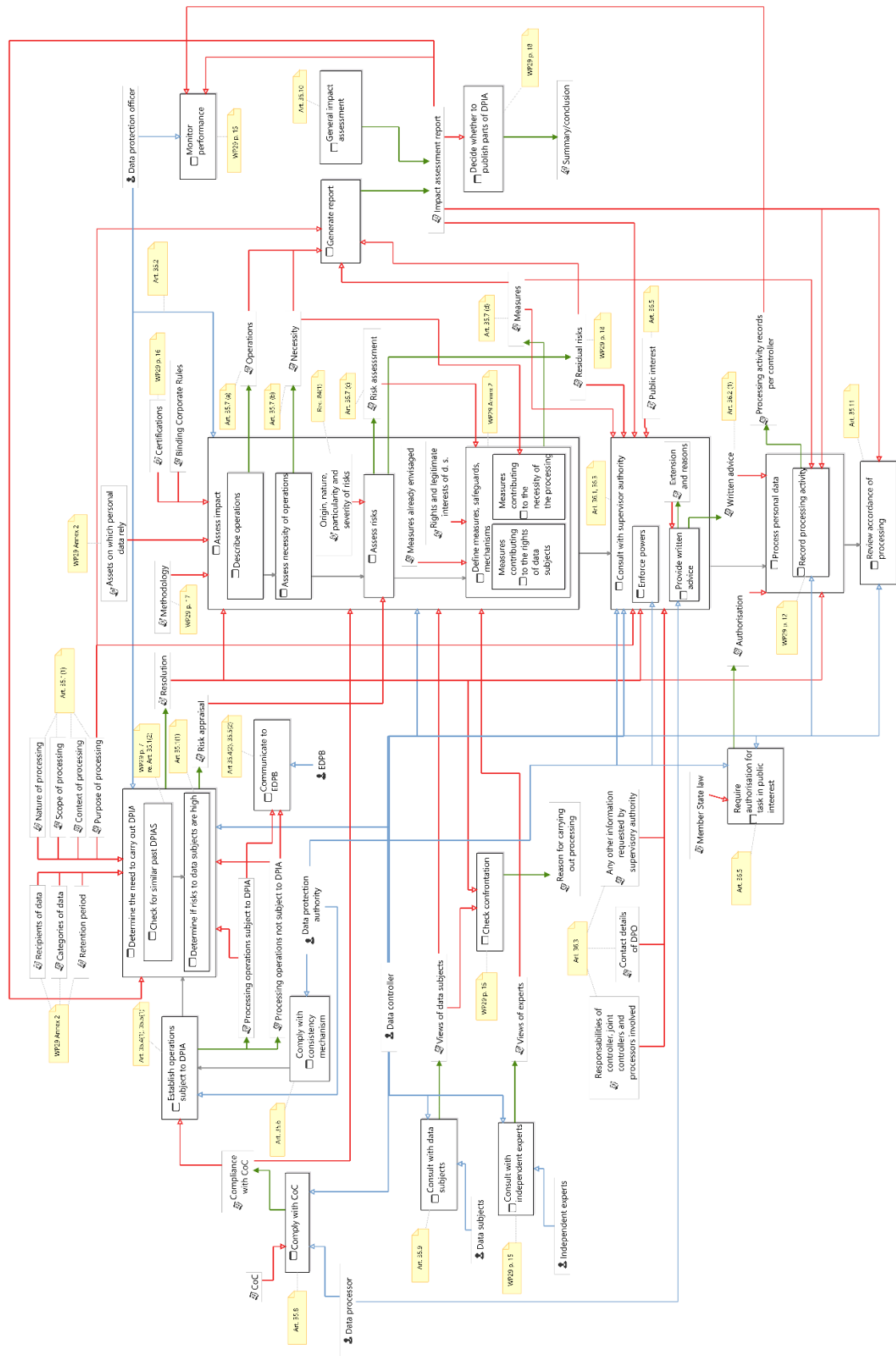









Figure 2. Reference Framework with the GDPR model.

4.3 Modelling approach and process

The model presented in Figure 2 above is too complex to create it in one go, even though it only covers two articles of the GDPR. Clearly, it cannot be created from scratch without a refined procedure underlying. In our case, we have applied a textual analysis of the contents of the GDPR (and other interpretative documents), an approach which is common in other disciplines such as requirements engineering or conceptual modelling, and which departs from a textual description of the system functions or concepts. In our case, we have used this approach to capture the elements of the process model underlying the execution of a DPIA, from its description in the GDPR. It shall be noted that, contrary to other kinds of documents such as ISO standards, GDPR, as a legal document, is not organized around a process description or list of detailed requirements and, thus, the extraction of the different process elements is not straightforward. The relation between the articles and the process stages is not linear, some elements are not described explicitly but implied by the text, etc.

Table 6 shows the notation that we have used (which resembles that of the diagrams, with our own additions), to introduce annotations in the text which codify different elements and relations, as well as the criteria employed to detect their appearance in the text.


Table 6. Codebook for annotation of Reference Framework and Argumentation Pattern elements and relations.

<p> activity</p> <p>which is discussed by the text or the given clause.</p> <p>It is usually a verb (or a verb phrase), typically introduced by a modal (e.g. shall or may) which establishes an obligation or a power.</p>
<p> artefact</p> <p>which is required as an input to the mentioned activity.</p> <p>It is typically introduced as a) the object (theme) of phrases such as “take into account”, b) the direct object of an activity defined by a communication or a transference verb.</p>
<p> artefact</p> <p>which is produced as a result of the mentioned activity.</p> <p>It is typically introduced as a) the object (theme or patient) of phrases such as “result into” or “contain”, b) the direct object of activities defined using other verbs.</p>
<p> role</p> <p>which carries out the said activity.</p> <p>It may appear as a) the agent of the activity (active verb subject or passive agent), b) the indirect object of the activity, c) mentioned as the provider of some “advice”, “accordance”, etc. which shall be provided to the main activity.</p>
<p> reference to another activity</p> <p>which is dependent on the execution of the current activity, which shall precede the referred activity.</p> <p>It is typically introduced by “prior to”, “before”, etc.</p>
<p> reference to another activity</p> <p>upon which the current activity depends, i.e. the current activity shall succeed the referred activity.</p> <p>It 1) is introduced by “already”, etc. or 2) mentions the results of the activity.</p> <p>The graphical notation is the same as in the previous case, the only difference is that the direction is reversed in relation to the current activity.</p>
<p> condition</p> <p>can represent different elements to be modelled in argumentation patterns (expressed using Goal Structuring Notation - GSN). At this stage, we don't</p>


distinguish among the different GSN elements that may be expressed by the text (goals, strategies, solutions, contexts, justifications, or assumptions), but just signal that a clause cannot be only modelled through the reference framework but it also requires an argumentation pattern. It should be noted, nonetheless, that the patterns defined from these conditions are not the only way to achieve a goal, they are just defining process patterns which offer one among several potential solutions.

A condition is usually identified by a conditional clause: 1) introduced by an interrogative adverb (“where”, “when”, “for which”), or 2) a conditional expression (“in the case of”, “subject to”, “unless”), or 3) directly an adverb phrase that sets some constraint (e.g. “in the public interest”). Sometimes, the conditions are quite generic (“where appropriate”, “where applicable”, “where necessary”). Sometimes, the condition can also be split into several parts in the text. The conditions may refer to artefacts, activities, or even roles, which can be omitted when some circumstances yield (e.g. the result of the DPO nomination may render that position unnecessary); but the negation of the premise established by the condition still validates the clause (e.g. when the DPO doesn’t exist, their participation in an activity is not required anymore).

WP29/EDPB guidance also provides complementary information that adds to many of the conditions established by GDPR.

[ *applicability constraints*] under which a given activity, role or artefact is required.








While the conditions mentioned (e.g. ‘processing is likely to produce a high risk’) and modelled using GSN shall be evaluated during the execution of an assurance project; the current applicability criteria (e.g. ‘the organization is an SME’, ‘there is a specific Member State law’), is already defined at the beginning of the assurance project.




[ *time constraints*] are not explicitly modelled yet, but truth is that they appear through GDPR. They might be modelled as evidence properties.

In the next subsections, we have included several tables with the annotated text of each clause of GDPR Art. 35 and 36, side to side to an explanation of why they have been modelled that way. Graphical excerpts depicting the respective clauses are also included, which zoom into details of the overall figure for the reference framework (Figure 2). Some independent figures are also provided as examples of argumentation patterns.

4.4 Model of Art. 35 Data protection impact assessment

Table 7. Annotated text of GDPR Art. 35.1 and 35.2.

<p>1. [ <i>Where a type of processing in particular using new technologies</i>], and taking into account the [ <i>nature</i>], [ <i>scope</i>], [ <i>context</i>] and [ <i>purposes</i>] of the processing, [ <i>... is likely to result in</i>] a [ <i>high risk to the rights and freedoms of natural persons</i>],</p>	<p>Note that this clause defines two activities:</p> <ul style="list-style-type: none"> - an implicit “Determination of the need to carry out a DPIA” (which produces an initial appraisal of the risk, plus a resolution on whether to proceed or not), and - the impact assessment itself (whose contents are detailed in later clauses). <p>The nature, scope, context and purpose of the processing are modelled elsewhere (using e.g. the methods described in D5.4 [15]). Other inputs</p>
--	--

<p>the [controller  →] shall, [▶ prior to the processing], <input type="checkbox"/> carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p>	<p>(e.g. recipients, categories, detailed guidance) are detailed in Annex 2 of WP29 guidance.</p> <p>The execution of the DPIA is only mandated under specific circumstances established by the condition (i.e. where a high risk is likely); this is modelled through an argumentation pattern, as explained in Section 2. Nonetheless, a DPIA can still be useful in any other cases, upon the decision of the data controller.</p> <p>The multiplicity aspect introduced by the last sentence is not explicitly modelled. Nonetheless, as WP29 guidance provides for the application of the same DPIA for similar Data processing purposes, a previous activity is introduced to check for previous, similar DPIAs. Given that determining that one DPIA is similar to another might not be trivial, we will consider the similarity analysis as a manual process out of the scope of this project. However, it does not preclude that certain elements will need to be introduced in the assurance case (even if those elements are manually generated), thus, it is not completely out of the scope of the assurance tool.</p>
<p>2. The [controller  →] shall seek the advice of the [data protection officer  →], [... ? where designated], <input type="checkbox"/> when carrying out a data protection impact assessment.</p>	<p>Adds the DPO as a (secondary) role to the impact assessment activity.</p> <p>As it may be the case that the DPO does not exist (it is not always required), a conditional clause is introduced (which is modelled as an argumentation pattern).</p>

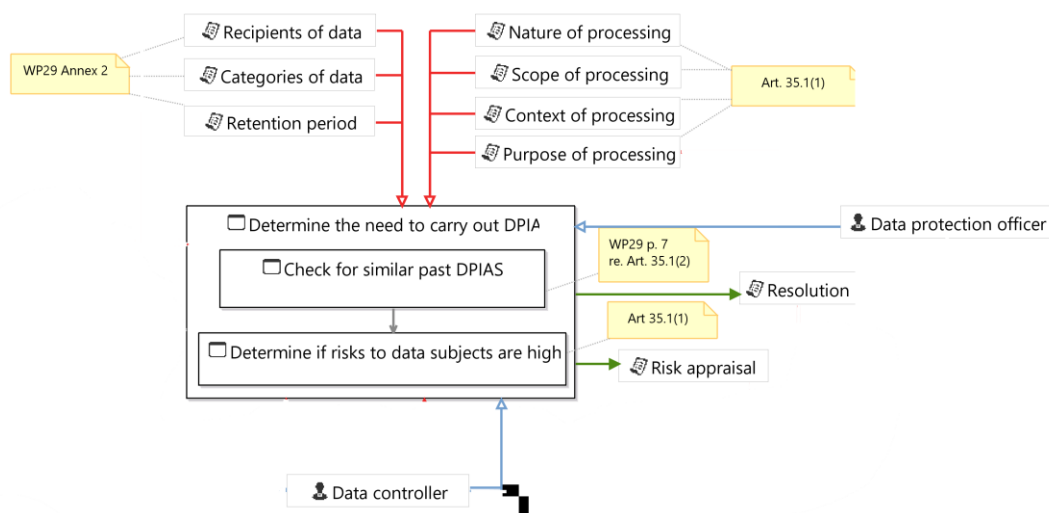


Figure 3. Reference framework modelling of GDPR Art. 35.1 and 35.2 (detail).

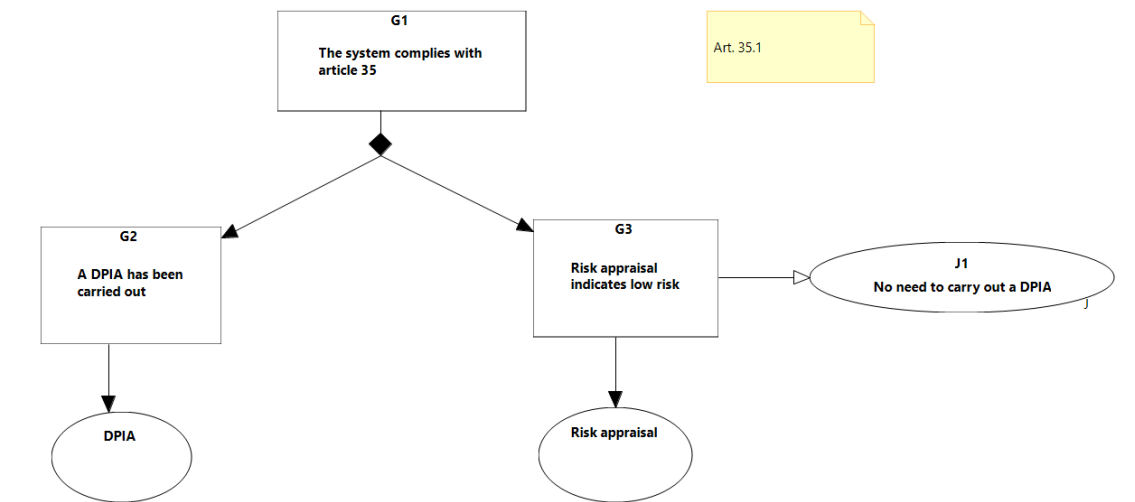








Figure 4. Argumentation pattern for Art. 35.1.

Table 8. Annotated text of GDPR Art. 35.3, 35.4 and 35.5.

<p>3. A [data protection impact assessment], referred to in paragraph 1 shall in particular be required <i>[?in the case of:</i></p> <ol style="list-style-type: none"> <i>a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;</i> <i>processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or</i> <i>a systematic monitoring of a publicly accessible area on a large scale.</i> <p><i>]</i></p>	<p>This clause provides details on when a DPIA is needed, which will be modelled through the refinement of the argumentation pattern. Recital 91, together with sections 3.B and 3.C of WP29 guidance [14] provide further details.</p>
<p>4. The [supervisory authority] shall [establish and make public] a [list of the kind of processing operations] <i>[?which are subject to the requirement]</i> for a [data protection impact assessment], pursuant to paragraph 1.</p> <p>The [supervisory authority] shall [communicate] [those lists] to the [Board] referred to in Article 68.</p>	<p>Two activities are defined: establishment of a list of operations and communication to the EDPB.</p> <p>Plus, the list of operations shall be used as an input to the DPIA, even if not explicitly listed as such. The argumentation pattern will keep refining the conditions under which a DPIA is required.</p>

<p>5. The [supervisory authority →] may also [<input type="checkbox"/> establish and make public] a [→ list of the kind of processing operations] [<i>?for which no data protection impact assessment is required</i>].</p>	The same as in the previous row.
<p>The [supervisory authority →] shall [<input type="checkbox"/> communicate] [those lists →] to the [Board →].</p>	
<p>6. [▶ Prior to the adoption of the lists] referred to in paragraphs 4 and 5, the competent [supervisory authority →] shall [<input type="checkbox"/> apply the consistency mechanism] referred to in Article 63 [<i>?where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.</i>]</p>	Depending on the contents of the list, the consistency mechanism will be required or not (thus, this clause is candidate for an argumentation pattern with a similar structure as others presented).

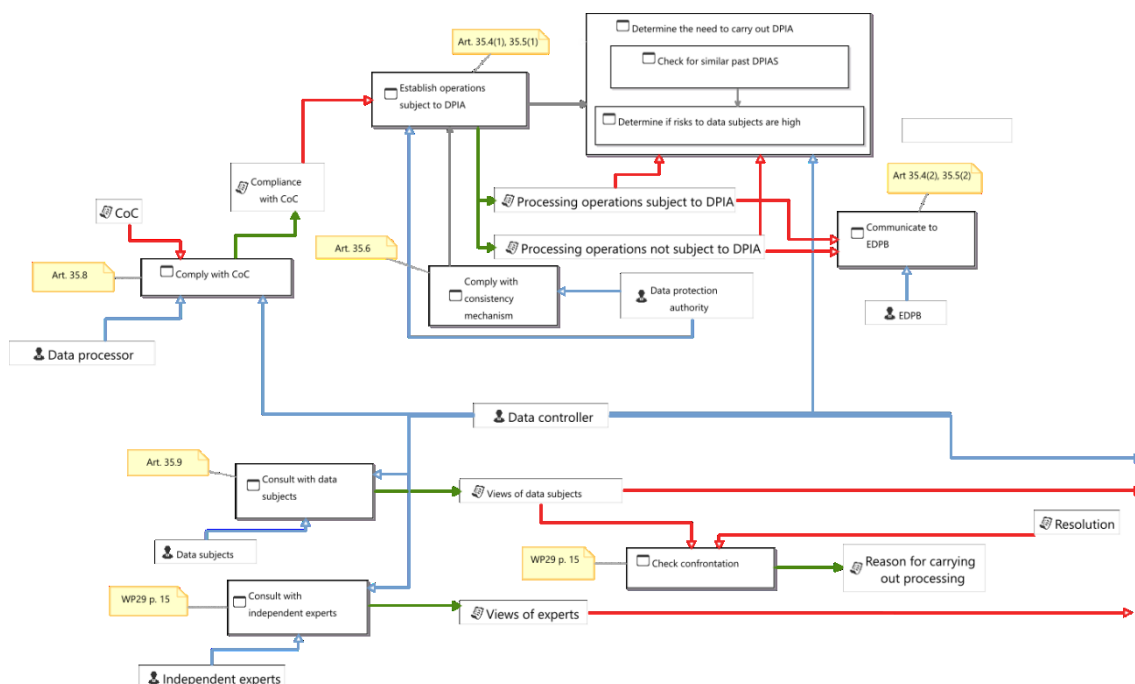






Figure 5. Reference framework modelling of GDPR Art. 35.4, 35.5, 35.6, 35.8 and 35.9 (detail).

Table 9. Annotated text of GDPR Art. 35.7 to 35.11.

<p>7. The [<input type="checkbox"/> assessment] shall contain at least:</p> <p>a) [→ a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller];</p>	<p>This clause specifies some of the outputs that must be created by the DPIA Activity (plus some inputs required).</p> <p>We decompose this activity into four sub-activities which respectively create each output. These sub-activities are not explicitly defined by GDPR, but they are implicitly required in order to</p>
---	---

<p>b) [→] an assessment of the necessity and proportionality of the processing operations in relation to the purposes];</p> <p>c) [→] an assessment of the risks to the rights and freedoms of data subjects] referred to in paragraph 1; and</p> <p>d) [→] the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation] taking into account [the rights and legitimate interests of data subjects and other persons concerned →].</p>	<p>create each artefacts. Indeed, we define requirements owned (i.e. post-conditions) by the overall privacy impact assessment activity, which then appear as constraining (i.e. satisfied) requirements by the output artefacts.</p> <p>Besides, it is useful to have these sub-activities explicitly specified, as then each one can be independently mapped to realizations defined by e.g. industry standards. (Note that GDPR doesn't tell how these outputs shall be produced, only that they are required; it's the role of industry to determine how they are created.)</p> <p>While paragraph c mentions the assessments of the risks, it does not detail which those risks are. An example of potential kinds of risks are the ones which are mentioned in Rec. 75, modelled through the argumentation pattern shown in Figure 7</p> <p>Other inputs and outputs to the impact assessment are specified by recital 84 and WP29 guidance.</p>
<p>8. [Compliance with approved codes of conduct →] referred to in Article 40 by the relevant [controllers →] or [processors →] shall be taken into due account in [□ assessing the impact of the processing operations performed by such controllers or processors], in particular for the purposes of a data protection impact assessment.</p>	<p>Compliance with Codes of Conduct (by both controllers and processors) is listed as another input for DPIAs. The activity "Comply with CoC" here is listed as a placeholder (see Figure 5 above), to be further developed in the modelling of the respective articles dealing with Codes of Conduct (Art. 40, etc.)</p>
<p>9. [? Where appropriate], the [controller →] shall [□ seek the views] of [data subjects or their representatives →] on the intended processing, [? without prejudice to the protection of commercial or public interests or the security of processing operations].</p>	<p>An additional activity involving the controller and the data subjects is modelled. WP29 guidance also provides for consultation with independent experts.</p> <p>An argumentation pattern will deal with the conditional clauses.</p>
<p>10. [? Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question], and [a data protection impact assessment has already been carried out ▶] as part of a [→] general impact assessment in the context of the adoption of that legal basis], [? paragraphs 1 to 7 shall not apply] [unless Member States deem it to be necessary] to [□ carry out such an assessment] [▶ prior to processing activities].</p>	<p>A "General impact assessment" (which also deals with data protection) is a perfect alternative to a specific DPIA, under some of the legal basis for processing, as specified.</p>

11. [? Where necessary], the [controller ] shall [ carry out a review to assess if processing is performed in accordance] with [ the data protection impact assessment] [? at least when there is a change of the risk represented by processing operations].

After the DPIA is carried out, data processing activities are held by the controller. Later, the impact assessment report shall be revised.

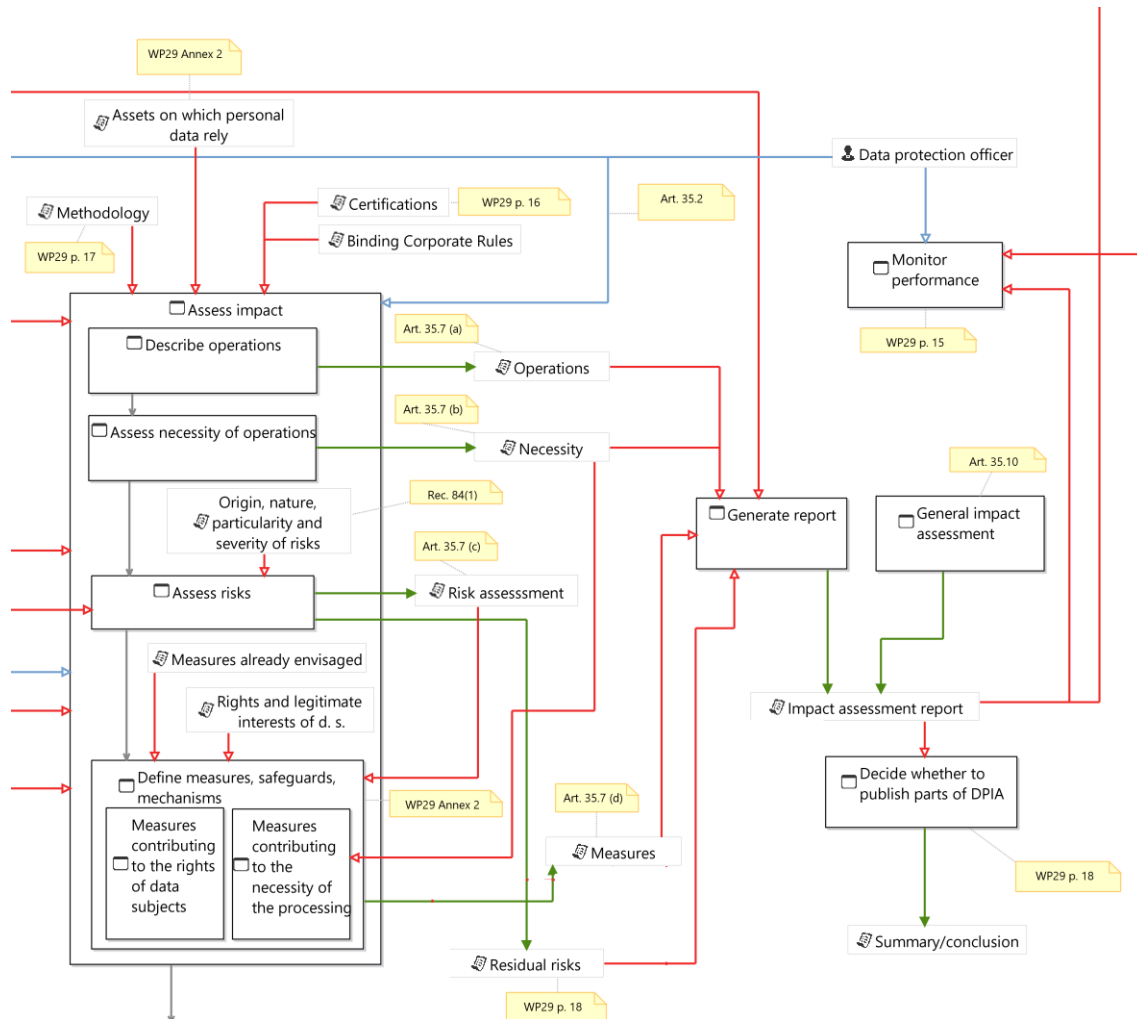


Figure 6. Reference Framework modelling of GDPR Art. 35.7 and 35.10 (detail).

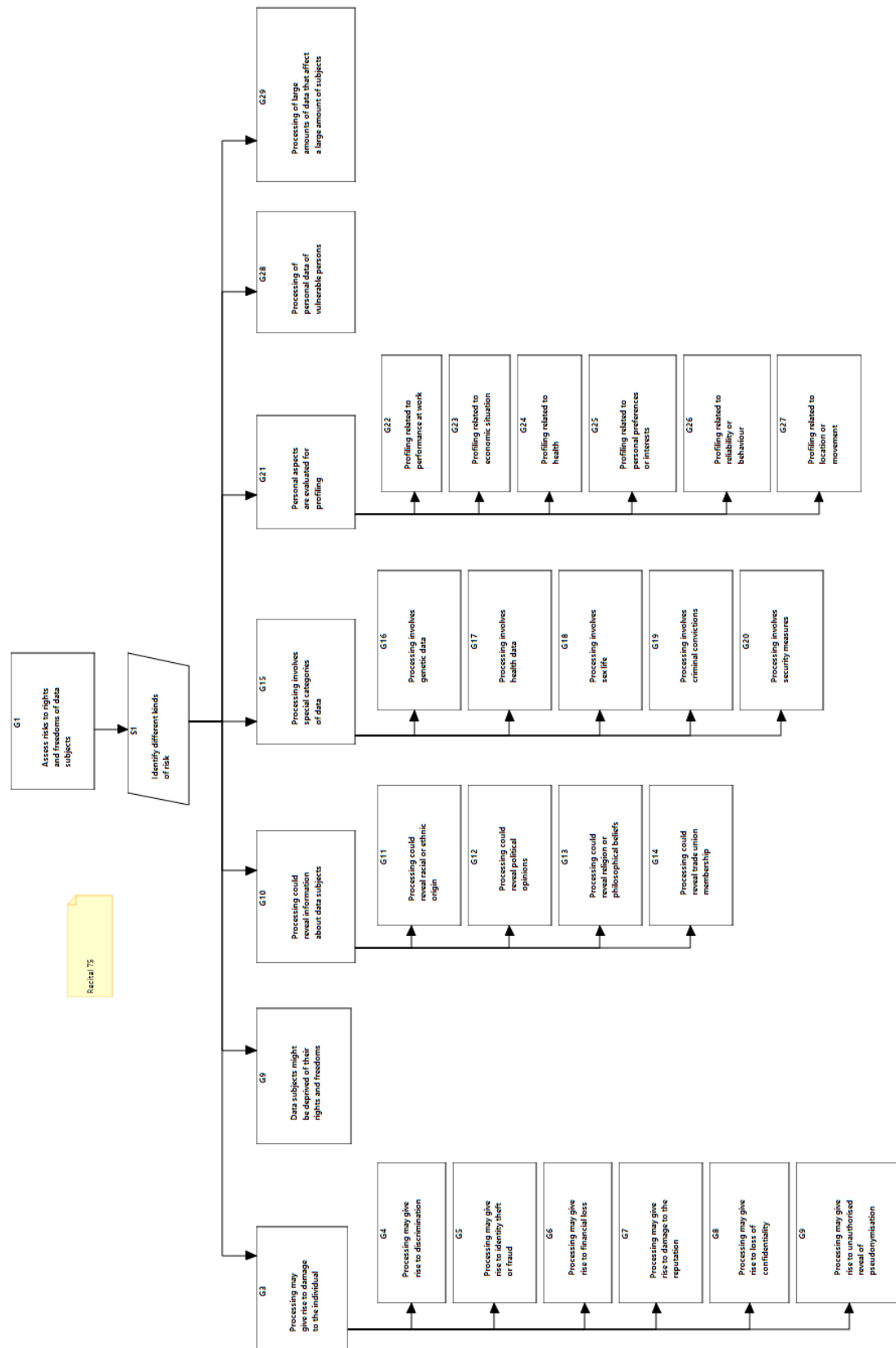
























Figure 7. Argumentation pattern modelling different risks sources as per GDPR recital 75 (landscape oriented).

4.5 Model of Art. 36 Prior consultation

<p>1. The [controller  →] shall [ consult] the [supervisory authority  →] [▶ prior to processing] [<i>? where</i>] [a data protection impact assessment ▶] under Article 35 [<i>... ? indicates that the processing would result</i>] in a [high risk  →] [<i>... ? in the absence of measures taken by the controller to mitigate the risk.</i>]</p>	<p>Consultation with DPA is explicitly modelled as a separate activity: it's not just that the DPA acts as an advisor in a given activity, but that a whole set of (sub-)activities and artefacts are specified.</p> <p>Precedence relations are set: consultation shall take place prior to processing and after the DPIA has been carried out.</p> <p>Inputs include the risk assessment (produced by the DPIA), plus others—as detailed in the next clauses—.</p>
<p>2. [<i>? Where</i>] the [supervisory authority  →] is of the opinion [<i>? that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk</i>], the [supervisory authority  →] shall, [ within period of up to eight weeks of receipt of the request for consultation], [ provide written advice] to the [controller  →] and, [<i>∇ where applicable</i>], to the [processor  →], and may [ use any of its powers] referred to in Article 58. [ That period may be extended by six weeks], [<i>? taking into account the complexity</i>] of [the intended processing  →]. The [supervisory authority  →] shall inform the [controller  →] and, [<i>∇ where applicable</i>], the [processor  →], of [ any such extension] [ within one month of receipt of the request for consultation] together with [ the reasons for the delay]. [ Those periods may be suspended until] the [supervisory authority  →] has obtained [information it has requested  →] for the purposes of the consultation.</p>	<p>The details of the consultation activity are provided. It may include two sub-activities: provide written advice and/or enforce powers. The written advice may be delayed; in that case, an artefact is created with the reasoned extension decision, and it is reused as an input for the same activity.</p> <p>More input artefacts are detailed here (in this case, they are later repeated in the next clause): details of processing activities, and any other information requested by the DPA.</p> <p>Note that timing constraints are not modelled, as they are not supported by the current version of the assurance tool.</p>

<p>3. When [consulting] the [supervisory authority] pursuant to paragraph 1, the [controller] shall provide the [supervisory authority] with:</p> <ul style="list-style-type: none"> a) <i>[where applicable]</i>, [the respective responsibilities of the controller, joint controllers and processors involved in the processing], <i>[in particular for processing within a group of undertakings]</i>; b) [the purposes and means of the intended processing]; c) [the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation]; d) <i>[where applicable]</i>, [the contact details of the data protection officer]; e) [the data protection impact assessment provided for in Article 35]; and f) [any other information] <i>[requested by the supervisory authority]</i>. 	<p>This clause deals with yet more inputs required for the consultation by the DPA from the controller: description of responsibilities of each role, purposes and means of processing, measures and safeguards taken, contact details of the DPO, the whole DPIA itself, plus any other information requested by the DPA.</p>
<p>4. [Member States] shall consult the [supervisory authority] during the [preparation] of a [proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure], <i>[which relates to processing]</i>.</p>	<p>Not modelled, as they go beyond the scope of Privacy and Data Protection Engineering.</p>
<p>5. Notwithstanding paragraph 1, <i>[Member State law may require]</i> [controller] to [consult] with, and [obtain prior] [authorisation] from, the [supervisory authority] <i>[in relation to processing]</i> by a [controller] for the performance of a task <i>[carried out by the controller in the public interest, including processing in relation to social protection and public health.]</i></p>	<p>Two activities whose descriptions are mingled:</p> <ol style="list-style-type: none"> 1) The consultation described by paragraph 1, for which new applicability constraints are introduced (when processing is carried out under public interest bases and there is a national law dictating so). 2) The obtention of an authorisation from DPA (required under the same circumstances). A precedence constraint is included, but it is split in the text ("obtain prior ... in relation to processing").

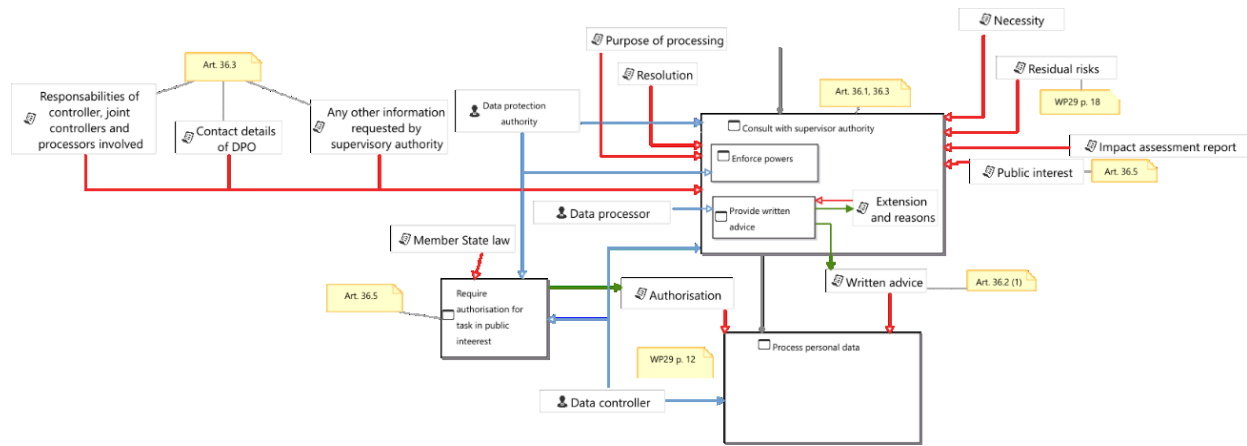


Figure 8. Reference framework modelling of GDPR Art. 36.1, 36.2, 36.3 and 36.5 (detail).

4.6 Modelling risk controls through argument patterns

Another assurance element that is part of the assurance knowledge database is the concept of the argument pattern used in assurance cases edition.

Assurance cases are a structured form of an argument that specifies convincing justification that a system is adequately dependable for a given application in a given environment. In this context argumentation patterns can be defined as a means of explicitly and clearly documenting common elements found between assurance cases. We have been working with two main areas of best practices specification for argument reuse, in one hand argument patterns in relation to the process followed complaining with GDPR and on the other hand product-based argumentation in relation with the controls implemented to mitigate vulnerabilities identified during the risk management process.

In the context of WP3, different controls from the NIST standard [11] are being discussed. As a result of the collaboration between the work packages, we have started with the design of argument patterns related to the risk controls implemented to mitigate or delete the vulnerabilities identified for the system. As a starting point the argumentation related to the SI-18 control is shown in Figure 9. As evidences proposed the outcomes from the system design are identified. The design of the system should follow the methodology proposed in WP4 and WP5 and the evidences expected here will be the outcomes of following those methods.

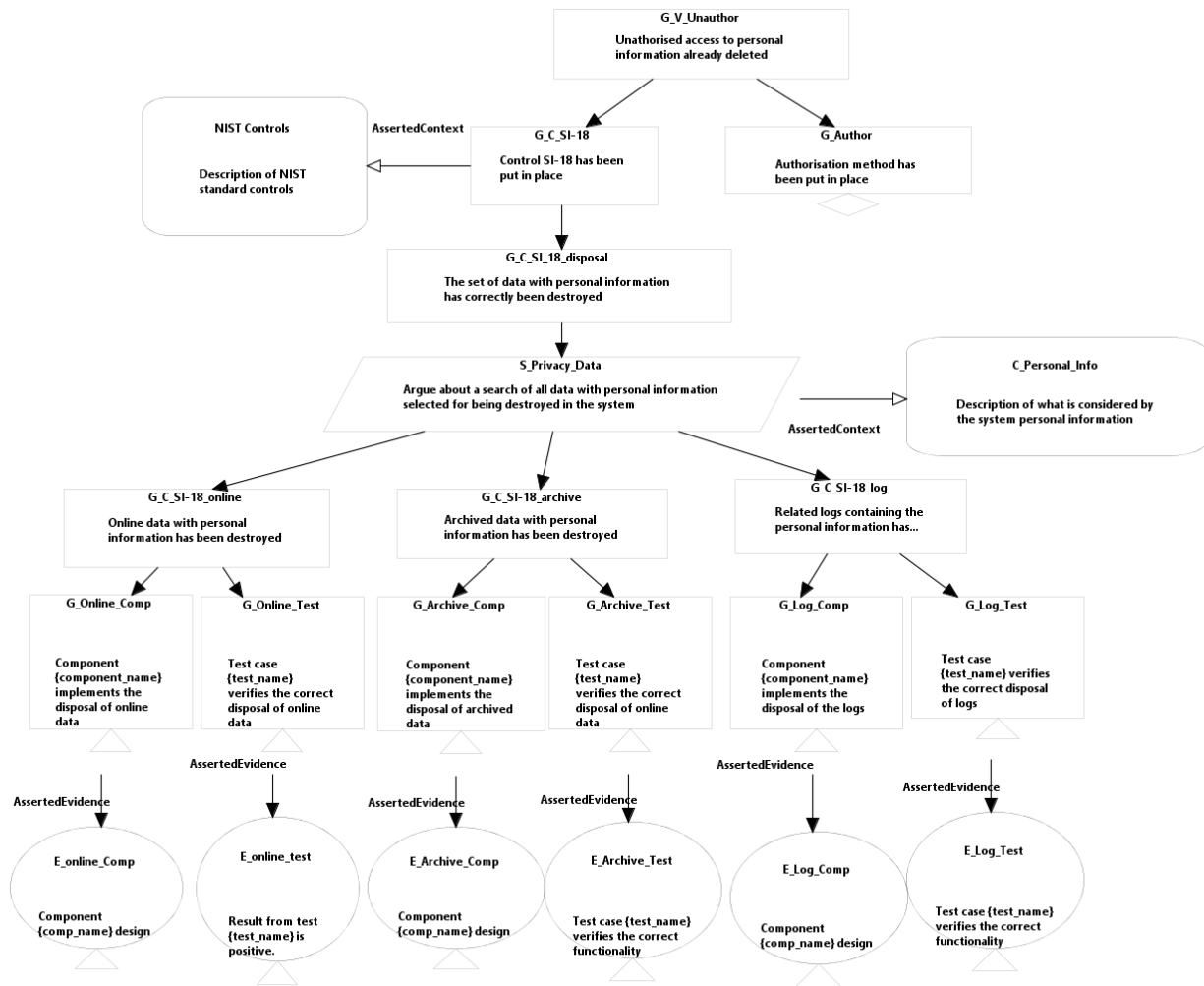


Figure 9. Argument pattern about the NIST control SI-18.

5 Conclusions

In this deliverable we have presented the preliminary method for assurance of privacy and data protection, with an especial focus on GDPR. Support to this method will be implemented in the assurance tool developed from OpenCert. We expect that future versions of the method will follow the same basic structure; however, we will advance the details of its content to cover a broader range of GDPR contents, besides further regulation that operationalizes its contents into engineering terms (e.g. ISO29134 for DPIAs or ISO 27552 for privacy controls). Likewise, we will reflect the results of the feedback from the validation from the demonstration scenarios.

6 References

- [1] PDP4E Project Deliverable; D2.2 Technical Gap Analysis and Synthesis of User Requirements; March 2019
- [2] North Atlantic Treaty Organization. Nato Standard AEP-67. Engineering For System Assurance In Nato Programmes, Edition B Version 1. October 2017. Nato Standardization Office (NSO, NATO/OTAN). Available at <https://nso.nato.int/nso/zPublic/ap/PROM/AEP-67%20EDB%20V1%20E.pdf>
- [3] Pierre Bourque, Richard E. (Dick) Fairley (eds.). Guide to the Software Engineering Body of Knowledge. Version 3.0. SWEBOK. IEEE, 2014. ISBN-13: 978-0-7695-5166-1 . Available from <https://www.computer.org/education/bodies-of-knowledge/software-engineering/v3>
- [4] Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services. Official Journal of the European Union, section L, issue 335, page 13, 21/12/2005.
- [5] Commission Implementing Regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010. Official Journal of the European Union, section L, issue 271, page 23, 18/10/2011.
- [6] M. Hansen, M. Jensen and M. Rost, "Protection Goals for Privacy Engineering," 2015 IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 159-166. doi: 10.1109/SPW.2015.13
- [7] M. Adedjouma, B. Botella, H. Espinoza, Zoe Stephenson, Marc Born, Muhammad Atif Javed, Faiz UL Muram, Nils Muellner, Barbara Gallina, Stefano Puri, Alejandra Ruiz, Angel López, Cristina Martinez. AMASS platform validation D2.9. AMASS Consortium. Available at https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/D2.9_AMASS-platform-validation_AMASS_Final.pdf
- [8] PDP4E Project Deliverable; D6.1 Specification and design of assurance tool dor data protection and privacy; July 2019.
- [9] Kühling, J., Martini, M., & Heberlein, J. (2016). *Die Datenschutz-Grundverordnung und das nationale Recht: erste Überlegungen zum innerstaatlichen Regelungsbedarf*. Monsenstein und Vannerdat. http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf
- [10] The Assurance Case Working Group (ACWG). Goal Structuring Notation Community Standard Version 2 SCSC-141B. January 2018.
- [11] NIST National Institute of Standards and Technology; "NIST SP 800-53, - Security and Privacy Controls for Information Systems and Organizations"
- [12] ISO/IEC 27701:2019 Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines. International Organization for Standardisation (ISO), August 2018.
- [13] Helmut Martin, Bernhard Winkler, Robert Bramberger, Muhammad Atif Javed, Faiz UI Muram, Irfan Slijivo, Barbara Gallina, Julieth Castellanos, Jose Luis de la Vara, Miguel Rozalen, Jose María Álvarez Universidad Carlos III de Madrid (UC3) Luis Alonso, Borja López, Elena Gallego, Alejandra Ruiz, Angel López, Huáscar Espinoza, Marc Sango, Staffan Skogby, Detlef Scholle, Jan Mauersberger. Methodological guide for cross/intra-domain reuse (b) D6.8. AMASS Consortium. Available at https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D6.8_Methodological-guide-for-cross-intra-domain-reuse-%28b%29_AMASS_Final.pdf
- [14] Article 29 Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248 rev. 01 As last Revised and Adopted on 4 October 2017. The Working Party on The Protection of Individuals With Regard to The Processing of Personal Data. Retrieved from https://ec.europa.eu/newsroom/document.cfm?doc_id=47711
- [15] PDP4E Project Deliverable. D5.4 Methods for Data Protection Model-Driven Design. August 2019.